UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,981	03/21/2005	Hisato Shima	265501US6PCT	4375

22850 7590 12/28/2007

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER
PACHURA, REBECCA L

ART UNIT	PAPER NUMBER
4171	

NOTIFICATION DATE	DELIVERY MODE
12/28/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/527,981	SHIMA ET AL.	
	Examiner	Art Unit	
	REBECCA L. PACHURA	4171	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *03/21/2005, 04/28/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-13 are presented for examination.**

The claims and only the claims form the metes and bounds of the invention. "Office personnel are to give claims their broadest reasonable interpretation in light of the supporting disclosure. In re Morris, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim are not read into the claim. In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA 1969)" (MPEP p 2100-8, c 2, I 45-48; p 2100-9, c 1, l 1-4). The Examiner has full latitude to interpret each claim in the broadest reasonable sense. The Examiner will reference prior art using terminology familiar to one of ordinary skill in the art. Such an approach is broad in concept and can be either explicit or implicit in meaning.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 03/21/2005 and 04/28/2006 are in compliance with the provisions of 37 CFR 1.97, except where lined through. The documents that are lined through were not considered because an English translation was not provided of the abstract or any other part of the document. Otherwise, the information disclosure statement is being considered by the examiner.

Preliminary Amendment

3. The preliminary amendment submitted on 03/21/2005 is duly noted.

Priority

4. The foreign priority claim of application # 2003-291971 JP of 08/12/2003 is duly noted.

Specification

5. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Applicant is reminded of the proper language and format for an abstract of the disclosure.

> The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.
>
> The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The abstract of the disclosure is objected to because it exceeds 150 words in length. Correction is required. See MPEP § 608.01(b).

The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Claim Objections

6. Claims 6 and 12 are objected to because of the following informalities: line 6 states *"application level or data based on the device address at the application level"* it should state *"application layer or data based on the device address at the application layer"*. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. **Claim 13 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.** *"A computer program for executing"* must be embodied in some sort of hardware. In view of the below sited MPEP section the claim is non-statutory because it is functional descriptive material per se.

> **MPEP 2106.01 [R-5]**
> Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).)
> Both types of "descriptive material" are nonstatutory when claimed as descriptive material per se, 33 F.3d at 1360, 31 USPQ2d at 1759.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 1-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over "A Secure Registration Protocol for Media Appliances in Wireless Home Networks" (Kumar) (Applicant's IDS) in view of US 20040117650 (Karaoguz) and in view of US 5757924 (Friedman).**

As to claim 1, Kumar discloses a communication processing apparatus for executing a communication process via a network, characterized in that: a communication process related to an authentication process according to a predetermined authentication method is performed in order to acquire secret information permitted to be disclosed only to devices in a local network

corresponding to said authentication method (Kumar page 110, column 2, lines 14-22: In this section, we describe the protocol in detail. The protocol aims IO provide secure bootstrap registration and secure connection establishment between the device and Actiway. The protocol enables and enforces these two parties to authenticate to each other. In addition, the protocol requires an explicit authorization from the user before a device can enter the network, and includes shared key distribution mechanism to establish a secure communications channel between ***Actiway*** and the device). Kumar fails to teach unique identification information of a communication destination device in said communication process is acquired by data processing at a network layer or lower of an OSI reference model; unique identification information of an authentication partner device is acquired in an authentication sequence of said authentication method as data processing at an application layer of the OSI reference model.

However, Karaoguz discloses unique identification information of a communication destination device in said communication process is acquired by data processing at a network layer or lower of an OSI reference model; unique identification information of an authentication partner device is acquired in an authentication sequence of said authentication method as data processing at an application layer of the OSI reference model (Karaoguz paragraph 0039, lines 5-8: …Specifically, the media exchange network 100 may be a communication network comprising a personal computer (PC) 101, a media processing system (MPS) 102, and at least one media peripheral (MP)…and paragraph 0043: …Each of the elements or components of the network for communicating media or media exchange network may be identified by a network protocol address or other identifier which may include, but is not limited to, an Internet protocol (IP) address, a media access control (MAC) address and an electronic serial number (ESN)…).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that both the authentication partner device and the communication destination device could be either a MAC address or an IP address (Karaoguz paragraph 0039, lines 5-8: …Specifically, the media exchange network 100 may be a communication network comprising a personal computer (PC) 101, a media processing system (MPS) 102, and at least one media peripheral (MP)…and paragraph 0043: …Each of the elements or components of the network for communicating media or media exchange network may be identified by a network protocol address or other identifier which may include, but is not limited to, an Internet protocol (IP) address, a media access control (MAC) address and an electronic serial number (ESN)…).

Kumar discloses said acquired unique identification information of said communication destination device is matched with said acquired unique identification information of said authentication partner device; and in accordance with a passed or failed state of the matching, a process is executed to judge whether said authentication partner device is a device connected to a same local network as a local network to which a local device being a communication source device is connected (Kumar page 111, column 2, lines 11-26: 1. Authentication of the media device to the AS: The device needs to identify and authenticate itself to the AS in order to show that it is genuine. Step I : The device broadcasts DevReq over the WAN to the gateway. This frame contains the device ID, the current value of the device counter (Dcount), and the HMAC record signed by the secret key (KMAC). Step 2: The gateway copies all information in the DevReq frame together with its gateway ID into a new message, called DevAut, and sends it to the AS via SSL. Step 3: Once the AS receives the DevAut message from the gateway, it first checks that the message is authentic by computing the HMAC record. If the result matches one

attached in the message, the AS accepts and trusts the device. The AS then notifies the gateway via the DevAutRes message that the device can be trusted).

As to claim 2, the modified Kumar discloses the communication processing apparatus as claimed in claim 1. Kumar discloses characterized that at least one of said unique identification information received from said authentication partner device is received as processed data generated by an encryption process or a hash value generation process based on secret information shared with said communication source device (Kumar page 110, column 2, lines 35-38 and page 111, column 1, lines 1-5: …such as public key encryption and digital signatures. Each device has a globally unique device ID, and into each device are embedded two secret keys (KE,KMAC) in a secured fashion. Authentication Server (AS) - The AS resides on the Internet and may be specific to device manufacturer. It maintains a unique identifier and access key (which the user obtains at the time of purchase) for each genuinely manufactured device. The AS also keeps a secure database of each device's embedded secret keys KE and KMAC. Initially when the device comes up on the network, both the device and Actiway do not trust each other. The AS mediates the establishment of trust and a secure channel between the device and Actiway).

As to claim 3, the modified Kumar discloses the communication processing apparatus as claimed in claim 1. The modified Kumar fails to teach characterized in that identification information received from said communication destination device is a node unique ID defined in IEEE 1394 standards.

However, Karaoguz discloses characterized in that identification information received from said communication destination device is a node unique ID defined in IEEE 1394 standards

(Karaoguz paragraph 0039, lines 12-15: …The MP 103 may interface with the PC 101 and/or the MPS 102 via, for example, a wireless link and/or a wired link. The wired link may be a USB or a Firewire (IEEE 1394) connection…).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that the MP interface is a destination device with a Firewire ID (Karaoguz paragraph 0039, lines 12-15: …The MP 103 may interface with the PC 101 and/or the MPS 102 via, for example, a wireless link and/or a wired link. The wired link may be a USB or a Firewire (IEEE 1394) connection…).

As to claim 4, the modified Kumar discloses the communication processing apparatus as claimed in claim 1. The modified Kumar fails to teach characterized in that: said communication processing apparatus is configured to receive, as identification information received from said communication destination device, identification information acquired from a PHY communication unit of said communication destination device and identification information acquired by a network communication unit of said communication destination device, and match a plurality of these identification information.

However, Karaoguz discloses characterized in that: said communication processing apparatus is configured to receive, as identification information received from said communication destination device, identification information acquired from a PHY communication unit of said communication destination device and identification information acquired by a network communication unit of said communication destination device, and match a plurality of these identification information (Karaoguz paragraph 0043, lines 5-8: …Specifically, the media exchange network 100 may be a communication network comprising a

personal computer (PC) 101, a media processing system (MPS) 102, and at least one media peripheral (MP)…and paragraph 0043: …Each of the elements or components of the network for communicating media or media exchange network may be identified by a network protocol address or other identifier which may include, but is not limited to, an Internet protocol (IP) address, a media access control (MAC) address and an electronic serial number (ESN)…).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that the electronic serial number is acquired from a media peripheral and is unique identification information from the physical layer (Karaoguz paragraph 0043, lines 5-8: …Specifically, the media exchange network 100 may be a communication network comprising a personal computer (PC) 101, a media processing system (MPS) 102, and at least one media peripheral (MP)…and paragraph 0043: …Each of the elements or components of the network for communicating media or media exchange network may be identified by a network protocol address or other identifier which may include, but is not limited to, an Internet protocol (IP) address, a media access control (MAC) address and an electronic serial number (ESN)…).

As to claim 5, the modified Kumar discloses the communication processing apparatus as claimed in claim 1. The modified Kumar fails to teach characterized in that identification information received from said communication destination device is a device address defined in communication standards.

However, Karaoguz discloses characterized in that identification information received from said communication destination device is a device address defined in communication standards (Karaoguz paragraph 0043, lines 5-8: …Specifically, the media exchange network 100 may be a communication network comprising a personal computer (PC) 101, a media processing

system (MPS) 102, and at least one media peripheral (MP)…and paragraph 0043: …Each of the elements or components of the network for communicating media or media exchange network may be identified by a network protocol address or other identifier which may include, but is not limited to, an Internet protocol (IP) address, a media access control (MAC) address and an electronic serial number (ESN)…).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that an IP address is a device address from a media peripheral (communication destination device) that is defined in a communication standard i.e. Internet Protocol address (Karaoguz paragraph 0043, lines 5-8: …Specifically, the media exchange network 100 may be a communication network comprising a personal computer (PC) 101, a media processing system (MPS) 102, and at least one media peripheral (MP)…and paragraph 0043: …Each of the elements or components of the network for communicating media or media exchange network may be identified by a network protocol address or other identifier which may include, but is not limited to, an Internet protocol (IP) address, a media access control (MAC) address and an electronic serial number (ESN)…).

As to claim 6, the modified Kumar discloses the communication processing apparatus as claimed in claim 1. The modified Kumar fails to teach characterized that said communication processing apparatus is configured to receive, as identification information received from said communication destination device, a device address as a source address of a packet transmitted from said communication destination device, and a device address stored in a packet by data processing at an application level or data based on the device address at the application level, and match a plurality of these device addresses.

However, Friedman discloses characterized that said communication processing apparatus is configured to receive, as identification information received from said communication destination device, a device address as a source address of a packet transmitted from said communication destination device, and a device address stored in a packet by data processing at an application level or data based on the device address at the application level, and match a plurality of these device addresses (Friedman column 1, lines 51-62, column 2, lines 4-8 and 31-35: …for transmitting communicated data in the form of a bitstream organized into one or more packets to another node and for receiving a packet from another node. If the host 10 is a host computer attached to a subnetwork which is an Ethernet, then the host will have one I/O port which is an Ethernet interface. A host which initially generates a packet for transmission to another node is called the source node and a host which ultimately receives the packet is called a destination node. Communication is achieved by transferring packets via a sequence of nodes including the source node, zero or more intermediary nodes, and the destination node… The IP layer typically includes an IP source address, an IP destination address, a checksum, and a hop count which indicates a number of hops in a multihop network. A physical layer header includes a MAC address (hardware address) of the source and a MAC address of the destination…. In an internet 100 which uses the IP protocol, the IP addresses of the source and destination nodes are placed in the packet header 42 by the source node. A node which receives a packet can identify the source and destination nodes by examining these addresses…).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that packets could contain source addresses and that checksums can match the device addresses (Friedman column 1, lines 51-62, column 2, lines 4-8 and 31-35: …for transmitting

communicated data in the form of a bitstream organized into one or more packets to another node and for receiving a packet from another node. If the host 10 is a host computer attached to a subnetwork which is an Ethernet, then the host will have one I/O port which is an Ethernet interface. A host which initially generates a packet for transmission to another node is called the source node and a host which ultimately receives the packet is called a destination node. Communication is achieved by transferring packets via a sequence of nodes including the source node, zero or more intermediary nodes, and the destination node… The IP layer typically includes an IP source address, an IP destination address, a checksum, and a hop count which indicates a number of hops in a multihop network. A physical layer header includes a MAC address (hardware address) of the source and a MAC address of the destination…. In an internet 100 which uses the IP protocol, the IP addresses of the source and destination nodes are placed in the packet header 42 by the source node. A node which receives a packet can identify the source and destination nodes by examining these addresses…).

As to claim 7, Kumar discloses a communication controlling method for executing a communication process via a network (Kumar page 110, column 2, lines 14-22: In this section, we describe the protocol in detail. The protocol aims IO provide secure bootstrap registration and secure connection establishment between the device and Actiway. The protocol enables and enforces these two parties to authenticate to each other. In addition, the protocol requires an explicit authorization from the user before a device can enter the network, and includes shared key distribution mechanism to establish a secure communications channel between ***Actiway*** and the device). Kumar fails to teach said method characterized by comprising: an identification information acquiring step of acquiring unique identification information of a communication

destination device in a communication process by data processing at a network layer or lower of an OSI reference model, and acquiring unique identification information of an authentication partner device in an authentication sequence of a predetermined authentication method as data processing at an application layer of the OSI reference model.

However, Karaoguz discloses said method characterized by comprising: an identification information acquiring step of acquiring unique identification information of a communication destination device in a communication process by data processing at a network layer or lower of an OSI reference model, and acquiring unique identification information of an authentication partner device in an authentication sequence of a predetermined authentication method as data processing at an application layer of the OSI reference model (Karaoguz paragraph 0039, lines 5-8: …Specifically, the media exchange network 100 may be a communication network comprising a personal computer (PC) 101, a media processing system (MPS) 102, and at least one media peripheral (MP)…and paragraph 0043: …Each of the elements or components of the network for communicating media or media exchange network may be identified by a network protocol address or other identifier which may include, but is not limited to, an Internet protocol (IP) address, a media access control (MAC) address and an electronic serial number (ESN)…).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that both the authentication partner device and the communication destination device could be either a MAC address or an IP address (Karaoguz paragraph 0039, lines 5-8: …Specifically, the media exchange network 100 may be a communication network comprising a personal computer (PC) 101, a media processing system (MPS) 102, and at least one media peripheral (MP)…and paragraph 0043: …Each of the elements or components of the network

for communicating media or media exchange network may be identified by a network protocol address or other identifier which may include, but is not limited to, an Internet protocol (IP) address, a media access control (MAC) address and an electronic serial number (ESN)…).

Kumar discloses a matching processing step of performing a matching of said acquired unique identification information of said communication destination device with said acquired unique identification information of said authentication partner device; and a judging step of judging, in accordance with a passed or failed state of the matching, whether said authentication partner device is a device connected to a same local network as a local network to which a local device being a communication source device is connected (Kumar page 111, column 2, lines 11-26: 1. Authentication of the media device to the AS: The device needs to identify and authenticate itself to the AS in order to show that it is genuine. Step I: The device broadcasts DevReq over the WAN to the gateway. This frame contains the device ID, the current value of the device counter (Dcount), and the HMAC record signed by the secret key (KMAC). Step 2: The gateway copies all information in the DevReq frame together with its gateway ID into a new message, called DevAut, and sends it to the AS via SSL. Step 3: Once the AS receives the DevAut message from the gateway, it first checks that the message is authentic by computing the HMAC record. If the result matches one attached in the message, the AS accepts and trusts the device. The AS then notifies the gateway via the DevAutRes message that the device can be trusted).

As to claim 8, the modified Kumar discloses the communication controlling method as claimed in claim 7, characterized in that in said identification information acquiring step, at least one of said unique identification information received from said authentication partner device is

received as processed data generated by an encryption process or a hash value generation process based on secret information shared with said communication source device (Kumar page 110, column 2, lines 35-38 and page 111, column 1, lines 1-5: …such as public key encryption and digital signatures. Each device has a globally unique device ID, and into each device are embedded two secret keys (KE,KMAC) in a secured fashion. Authentication Server (AS) - The AS resides on the Internet and may be specific to device manufacturer. It maintains a unique identifier and access key (which the user obtains at the time of purchase) for each genuinely manufactured device. The AS also keeps a secure database of each device's embedded secret keys KE and KMAC. Initially when the device comes up on the network, both the device and Actiway do not trust each other. The AS mediates the establishment of trust and a secure channel between the device and Actiway).

As to claim 9, the modified Kumar discloses the communication controlling method as claimed in claim 7. The modified Kumar fails to teach characterized in that identification information received from said communication destination device is a node unique ID defined in IEEE 1394 standards.

However, Karaoguz discloses characterized in that identification information received from said communication destination device is a node unique ID defined in IEEE 1394 standards (Karaoguz paragraph 0039, lines 12-15: …The MP 103 may interface with the PC 101 and/or the MPS 102 via, for example, a wireless link and/or a wired link. The wired link may be a USB or a Firewire (IEEE 1394) connection…).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that the MP interface is a destination device with a Firewire ID (Karaoguz paragraph

0039, lines 12-15: …The MP 103 may interface with the PC 101 and/or the MPS 102 via, for example, a wireless link and/or a wired link. The wired link may be a USB or a Firewire (IEEE 1394) connection…).

As to claim 10, the modified Kumar discloses the communication controlling method as claimed in claim 7. The modified Kumar fails to teach characterized in that said identification information acquiring step is a step of receiving, as identification information received from said communication destination device, identification information acquired from a PHY communication unit of said communication destination device and identification information acquired by a network communication unit of said communication destination device, and said matching processing step matches a plurality of these identification information.

However, Karaoguz discloses characterized in that said identification information acquiring step is a step of receiving, as identification information received from said communication destination device, identification information acquired from a PHY communication unit of said communication destination device and identification information acquired by a network communication unit of said communication destination device, and said matching processing step matches a plurality of these identification information (Karaoguz paragraph 0043, lines 5-8: …Specifically, the media exchange network 100 may be a communication network comprising a personal computer (PC) 101, a media processing system (MPS) 102, and at least one media peripheral (MP)…and paragraph 0043: …Each of the elements or components of the network for communicating media or media exchange network may be identified by a network protocol address or other identifier which may include, but is not

limited to, an Internet protocol (IP) address, a media access control (MAC) address and an electronic serial number (ESN)…).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that the electronic serial number is acquired from a media peripheral and is unique identification information from the physical layer (Karaoguz paragraph 0043, lines 5-8: …Specifically, the media exchange network 100 may be a communication network comprising a personal computer (PC) 101, a media processing system (MPS) 102, and at least one media peripheral (MP)…and paragraph 0043: …Each of the elements or components of the network for communicating media or media exchange network may be identified by a network protocol address or other identifier which may include, but is not limited to, an Internet protocol (IP) address, a media access control (MAC) address and an electronic serial number (ESN)…).

As to claim 11, the modified Kumar discloses the communication controlling method as claimed in claim 7. The modified Kumar fails to teach characterized in that identification information received from said communication destination device is a device address defined in communication standards.

However, Karaoguz discloses characterized in that identification information received from said communication destination device is a device address defined in communication standards (Karaoguz paragraph 0043, lines 5-8: …Specifically, the media exchange network 100 may be a communication network comprising a personal computer (PC) 101, a media processing system (MPS) 102, and at least one media peripheral (MP)…and paragraph 0043: …Each of the elements or components of the network for communicating media or media exchange network may be identified by a network protocol address or other identifier which may include, but is not

limited to, an Internet protocol (IP) address, a media access control (MAC) address and an electronic serial number (ESN)…).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that an IP address is a device address from a media peripheral (communication destination device) that is defined in a communication standard i.e. Internet Protocol address (Karaoguz paragraph 0043, lines 5-8: …Specifically, the media exchange network 100 may be a communication network comprising a personal computer (PC) 101, a media processing system (MPS) 102, and at least one media peripheral (MP)…and paragraph 0043: …Each of the elements or components of the network for communicating media or media exchange network may be identified by a network protocol address or other identifier which may include, but is not limited to, an Internet protocol (IP) address, a media access control (MAC) address and an electronic serial number (ESN)…).

As to claim 12, the modified Kumar discloses the communication controlling method as claimed in claim 7. The modified Kumar fails to teach characterized in that: said identification information acquiring step receives, as identification information received from said communication destination device, a device address as a source address of a packet transmitted from the communication destination device, and a device address stored in a packet by data processing at the application level or data based on the device address at the application level, and said matching processing step matches a plurality of these device addresses.

However, Friedman discloses characterized in that: said identification information acquiring step receives, as identification information received from said communication destination device, a device address as a source address of a packet transmitted from the

communication destination device, and a device address stored in a packet by data processing at the application level or data based on the device address at the application level, and said matching processing step matches a plurality of these device addresses (Friedman column 1, lines 51-62, column 2, lines 4-8 and 31-35: …for transmitting communicated data in the form of a bitstream organized into one or more packets to another node and for receiving a packet from another node. If the host 10 is a host computer attached to a subnetwork which is an Ethernet, then the host will have one I/O port which is an Ethernet interface. A host which initially generates a packet for transmission to another node is called the source node and a host which ultimately receives the packet is called a destination node. Communication is achieved by transferring packets via a sequence of nodes including the source node, zero or more intermediary nodes, and the destination node… The IP layer typically includes an IP source address, an IP destination address, a checksum, and a hop count which indicates a number of hops in a multihop network. A physical layer header includes a MAC address (hardware address) of the source and a MAC address of the destination…. In an internet 100 which uses the IP protocol, the IP addresses of the source and destination nodes are placed in the packet header 42 by the source node. A node which receives a packet can identify the source and destination nodes by examining these addresses…).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that packets could contain source addresses and that checksums can match the device addresses (Friedman column 1, lines 51-62, column 2, lines 4-8 and 31-35: …for transmitting communicated data in the form of a bitstream organized into one or more packets to another node and for receiving a packet from another node. If the host 10 is a host computer attached to a

subnetwork which is an Ethernet, then the host will have one I/O port which is an Ethernet interface. A host which initially generates a packet for transmission to another node is called the source node and a host which ultimately receives the packet is called a destination node. Communication is achieved by transferring packets via a sequence of nodes including the source node, zero or more intermediary nodes, and the destination node… The IP layer typically includes an IP source address, an IP destination address, a checksum, and a hop count which indicates a number of hops in a multihop network. A physical layer header includes a MAC address (hardware address) of the source and a MAC address of the destination…. In an internet 100 which uses the IP protocol, the IP addresses of the source and destination nodes are placed in the packet header 42 by the source node. A node which receives a packet can identify the source and destination nodes by examining these addresses…).

As to claim 13, Kumar discloses a computer program for executing a communication process via a network, said program characterized by comprising. Kumar fails to teach an identification information acquiring step of acquiring unique identification information of a communication destination device in a communication process by data processing at a network layer or lower of an OSI reference model, and acquiring unique identification information of an authentication partner device in an authentication sequence of a predetermined authentication method as data processing at an application layer of the OSI reference model.

However, Karaoguz discloses an identification information acquiring step of acquiring unique identification information of a communication destination device in a communication process by data processing at a network layer or lower of an OSI reference model, and acquiring unique identification information of an authentication partner device in an authentication

sequence of a predetermined authentication method as data processing at an application layer of the OSI reference model (Karaoguz paragraph 0039, lines 5-8: …Specifically, the media exchange network 100 may be a communication network comprising a personal computer (PC) 101, a media processing system (MPS) 102, and at least one media peripheral (MP)…and paragraph 0043: …Each of the elements or components of the network for communicating media or media exchange network may be identified by a network protocol address or other identifier which may include, but is not limited to, an Internet protocol (IP) address, a media access control (MAC) address and an electronic serial number (ESN)…).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that both the authentication partner device and the communication destination device could be either a MAC address or an IP address (Karaoguz paragraph 0039, lines 5-8: …Specifically, the media exchange network 100 may be a communication network comprising a personal computer (PC) 101, a media processing system (MPS) 102, and at least one media peripheral (MP)…and paragraph 0043: …Each of the elements or components of the network for communicating media or media exchange network may be identified by a network protocol address or other identifier which may include, but is not limited to, an Internet protocol (IP) address, a media access control (MAC) address and an electronic serial number (ESN)…).

Kumar discloses a matching processing step of performing a matching of said acquired unique identification information of said communication destination device with said acquired unique identification information of said authentication partner device; and a judging step of judging, in accordance with a passed or failed state of the matching, whether said authentication partner device is a device connected to a same local network as a local network to which a local

device being a communication source device is connected (Kumar page 111, column 2, lines 11-26: 1. Authentication of the media device to the AS: The device needs to identify and authenticate itself to the AS in order to show that it is genuine. Step I: The device broadcasts DevReq over the WAN to the gateway. This frame contains the device ID, the current value of the device counter (Dcount), and the HMAC record signed by the secret key (KMAC). Step 2: The gateway copies all information in the DevReq frame together with its gateway ID into a new message, called DevAut, and sends it to the AS via SSL. Step 3: Once the AS receives the DevAut message from the gateway, it first checks that the message is authentic by computing the HMAC record. If the result matches one attached in the message, the AS accepts and trusts the device. The AS then notifies the gateway via the DevAutRes message that the device can be trusted).

Prior Art

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US 200200777986 is pertinent because it teaches … techniques are provided for controlling and managing digital assets…

US 20030110229 is pertinent because it teaches …an apparatus for controlling transmission of data packets in an information network comprises a Regional Transaction Processor (RTP) operable to communicate with a Data Enabling Device (DED) and at least one workstation. The DED searches data packets for content match information…

US 20040117659 is pertinent because it teaches …systems and methods that prevent unauthorized access in a communications network are provided. In one embodiment, a system that prevents unauthorized access to a network device may include, for example, a network device and a headend. The headend may be coupled to a communications network. The network device may be deployed in a home environment and may be communicatively coupled to the communications network via the headend. The headend may be adapted, for example, to determine whether a request to access the network device is authorized…

US 20040268153 is pertinent because it teaches …a method and system are provided for allowing a user to efficiently manage communications. A system for allowing a user having a unique identity is provided, wherein the unique identity is associated with a plurality of electronic devices…

US 20050022015 is pertinent because it teaches …a conditional access system comprising a plurality of devices interconnected in a network, the devices being grouped in a first group and a second group, the devices of the first group operating in accordance with a first security framework and the devices of the second group operating in accordance with a second security framework, each device operating using a particular middleware layer, said middleware layer being arranged to authenticate another middleware layer of another device, said middleware layer being authenticated by the security framework in accordance with which the device operates...

US 7100199 is pertinent because it teaches …the present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic

appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information...

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to REBECCA L. PACHURA whose telephone number is (571)270-3402. The examiner can normally be reached on Monday-Thursday 7:30 am-6:00 pm est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ramesh Patel can be reached on (571) 272-3688. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/R. L. P./
/Rebecca L Pachura/
Examiner, Art Unit 4171

/Ramesh B. Patel/
Supervisory Patent Examiner, Art Unit 4171